Naval War College Review

Volume 65
Number 4 *Autumn*

Article 20

2012

In My View

Rex A. Buddenberg
Naval Postgraduate School

IN MY VIEW

SOME CAREFUL DEFINITIONS

Sir:

The *Naval War College Review* for Spring 2012 contains the article "Networking the Global Maritime Partnership." The subject is important and overdue. Unfortunately the article suffers from an egregious lack of definition discipline that makes the article full of faults and, in particular, gets to an ineffective end for our allies. (Sloppy terminology is endemic to the information technology business, both in and out of the Navy, so this is nothing new.)

The article makes three statements that I fully agree with:

- One is in the conclusion: "It is beyond debate that the U.S. Navy will continue to partner with other navies."
- The second is a page earlier: "The way forward may be easier than some think." This needs to be exploited, but the article is silent regarding it.
- And the nub of the shortcomings: "Interoperability does not fit into any requirements 'bin.'" We corporately do not know how to measure interoperability or improve it.

Unfortunately, the treatment does not show how these second or third points are to be achieved, either by the U.S. Navy itself or with its partner services or allies. The quotations given (one repeated below) by Vice Admiral Arthur K. Cebrowski are over a decade old—shouldn't we be making some more intellectual progress?

The hit parade of badly defined terms appears all over in the article. But the worst is the term "network" itself! If you google around a bit in a few dictionaries and program glossaries (or, in DODAF language, the TV2), you'll find dozens of definitions of the term "network," but two are sufficient here:

- *Communications network* (or internetwork) is one definition (and the one that the Canadians seem to be using in their legitimate complaint—"Is there a place for small navies?"). A communications network is "plumbing."

Naval War College Review, Vol. 65 [2012], No. 4, Art. 20

A communications network does not include end systems that generate or consume data; a communications network only transports the data. ARPANET was an example, so is SIPRNET, so are LANs in our ships. So is the extension of SIPRNET onto the battlefield in the USMC WPPL program. But we seem to lack an intra–battle group extension of the Internet which our allies' ships could plug into when sailing in company.

- *Information-systems networks* include the end systems (clients and servers, in the IT parlance) that attach to the communications system. The sense, decide, and act nodes are included in this definition.

In the case of this information-systems-network definition, the communications network is an absolutely necessary prerequisite. In the commercial world, most of the conversation on information-system networks (last year's buzz phrase was "SOA," service-oriented architecture, and this year's buzz phrase is "cloud computing") tacitly assumes an ample communications network. But this is not the case in the Navy, where at least one of the sense/decide/act nodes is on a different platform. Neither the assumption nor the fact can be taken for granted. But the article blithely does just that. So we're locked onto the superstructure, sans keel and hull.

Examples. There are information systems all around us. Warships have sensors (such as radars and lookouts), decision nodes (combat information centers), and actors (the warship's weapons), all connected together with some form of communications, which we generically call "local area networks." But we do not need to get exotic; our own nervous systems are classical information systems—sensory nerves, a decision node, and motor nerves to actuate muscles. All connected together by the axons—the communications system.

Complexity in information systems involves nesting and chaining of these same components. Usually when you take apart something advertised as SOA, you find lots of chaining. Mercifully, the authors did not use the much-abused and never-defined term "system of systems" in this article.

Admiral Cebrowski and John Garstka are quoted: "Network-centric warfare derives its power from . . . strong networking." Which definition is being used? The difference is not important in visionary statements, but it makes a lot of programmatic, interoperability, and infrastructure impact, and nowhere is it more critical than in cross-platform, cross-service, and cross-nation integration.

The program implication is that we have a dismal record in delivering information-system networks (including communications) within a single program, especially if the program crosses platform boundaries—which is always the case in interesting situations and is certainly the case in the integration of partner navies. The only programs that we've seemed to deliver correctly are those that

focus on a building block (such as GIG-BE, delivering the terrestrial-WAN backbone, limiting scope to the terminal router). A modularization model—how to fit the building blocks together—not only will benefit our allies but will improve our acquisition record.

There are a host of other terms in the article that have either no definition or myriad definitions:

- "Network-centric warfare" is used repeatedly but is not defined. Of note, "network-centric systems engineering" never appears at all. Network-centric systems engineering is simply attaching all end systems to a (communications) network (rather than to each other, point to point). This relaxes scale and modularity constraints. Network-centric systems engineering is a prerequisite to network-centric operations.
- Copernicus and FORCENet are both concepts or visions but are erroneously described as programs or are assumed to lead directly to programs. Global Command and Control System–Maritime was the program that emerged from Copernicus. What we today call GCCS-M is the result of the collapsing of no fewer than twenty-four tactical decision-support programs within SPAWAR alone into one, circa 1990.
- "Architecture" is used several times but not defined. Having been a "C3I architect" once in a former life, I'm well versed in 101 definitions of the term. Buried in here is the key to meeting complaints like the Canadians'. The authors state that "interoperability does not fit into any requirements 'bin,'" a statement I fully agree with. But without parsing interoperability into communications, data, process, procedure, cognitive, and doctrinal components, we have no means to measure it. Without measurement, we can't improve it. Interoperability is supposed to be the province of architecture, but modularization does not appear in the article. It is in no way clear that the requirements meetings described (e.g., AG-1, AG-6, etc.) will lead to a proper modularization model. We have no track record of success here.
- GIG has a definition—an evil PowerPoint one. Unfortunately it's worse than useless. Modularization is not spoken here.

To integrate our allies, we both need interoperability. Some of the infrastructure, such as a LAN in a ship, will be brought to the fleet by the national navy, not provided by the United States. So approaches of "buy into our infrastructure," such as "buy into Cooperative Engagement Capability (CEC)," are not appropriate.

The authors state, "The way forward may be easier than some think." They are right. Let's explore, using the first, communications-network, definition. The communications network is application-agnostic, and it is a prerequisite to the

Naval War College Review, Vol. 65 [2012], No. 4, Art. 20

applications (information system networks). So it must come before discussions like SOAs, but it will not prejudice those discussions. The communications internetwork is made up of three "plumbing" parts:

- A terrestrial-WAN (in the U.S. DoD, this is provided by the Defense Information System Network). DISN is made up of technology identical to that in commercial ISP infrastructure.
- LANs within platforms. The end systems in the platform attach to these LANs.
- Radio-WANs that interconnect the ships and connect them to the shoreside terrestrial-WAN.

The "glue" that routes these network segments together in the U.S. Navy is made up of quite ordinary (COTS) routers procured under the ADNS program.

All of these components except the radio-WAN can be acquired somewhat independently by a partner navy. And they may be procured on the open market —there are multiple suppliers. There is very little military-specific in the U.S. Navy's infrastructure. And none of a partner navy's need be either.

The radio-WAN landscape in the U.S. military has lain under a heavy fog for over a decade. The requirements term of the Joint Tactical Radio System program has been "interoperable radio," but never was "interoperability" defined as *ability to extend the Internet*. Sloppy definition, and consequently faulty requirements and scope, doomed the acquisitions. Meanwhile, the means to solve the problem have appeared in the commercial marketplace, and both the U.S. Marine Corps and the Army have found and deployed them on the battlefield. In Navy terms, we need the ability to extend the Internet, first from the routers at the communications stations (terminal nodes of the terrestrial-WAN ashore) to our ships, and second between the routers of the ships in the battle group (what we used to call "intra–battle group communications"). From the allied perspective, our partners need to know what the interface definition is.

The protocols necessary to do this have been standardized in the IEEE 802.16 and the TIA Long Term Evolution standards; adaptations from commercial practice are necessary only in the RF component (known as "Phy," for "physical media dependent"), not the protocols. Implementations exist from multiple vendors on the open market (ironically, the Marine Corps purchases were from a Canadian company). If you have a cell phone advertised as "4G" in your pocket, you have one of these standards implemented in it.

End systems need interface principles too. This principle applies to the interface; it is agnostic about the function of the end system. Principle: all end systems attach to a LAN within the platform. This applies, of course, to your laptop,

but it also applies to the decision-support equipment in CIC and to the radars, sonars, and other sensors in a warship. The corollary to this principle is that the data emitted by an end system must be secured before it leaves that end system; relying on the communications infrastructure to provide for authenticity and confidentiality of the data is not tenable in a coalition environment.

Discipline in the terminology is just as important as discipline in the modularization. The commercial information technology constantly overhypes the 1,001 applications that work over the Internet, in an effort to separate buyers from their money. As stewards of the nation's security and the taxpayers' money, we cannot uncritically reuse the terminology without some careful definitions.

REX A. BUDDENBERG
Senior Lecturer, Information Sciences Department
Naval Postgraduate School, Monterey, California